Science & Technology Facilities Council
Rutherford Appleton Laboratory

A Flexible Component based Access Contr
Architecture for OPeNDAP Servic

Philip Kershaw

STFC Rutherford Appleton Laboratory

British Atmospheric Data Centre
NATIONAL CENTRE FOR ATMOSPHERIC SCIENCE
NATURAL ENVIRONMENT RESEARCH COUNCIL

NEODC

Centre for Envir ntal Data Archival
SCIENCE AND TECHNOLOGY S COUNCIL
NATURAL ENVIRONMENT R OUNCIL

Background Themes

- Focus on two areas alluded to in the abstract:

1) *"Without ready means to restrict access to data for such services, data providers and data owners are constrained from making their data more widely available."*
   - Paradox: provision of access control can open access?!
     - illustrated by the BADC and OPeNDAP
   - But in the wider context of changing attitudes: data.gov.uk

2) *"The range of different security technologies available can make interoperability between services and user client tools a challenge."*
   - Vision of seamless access can seem remote:
   - Services too complicated, get in the way or simply broken
   - A need for flexible approach to enable support for different technologies

Inception

- Seeds planted with discussion started at this conference last year
- Solution based on the use of HTTP redirects
- OPeNDAP implementations have existing support for this*:
  1. Initiate request,
  2. server side security challenge
  3. Redirect to authentication endpoint
  4. Redirect authenticated client back to original requested URI
- NERC DataGrid Security and Python WSGI middleware
  - Security filter components arranged to give the desired access control configuration

* TDS: http://www.unidata.ucar.edu/projects/THREDDS/tech/reference/RestrictedAccess.html
PyDAP: http://pydap.org/client.html

Alternative Approaches to Authentication

- Why use redirects at all? Host service over HTTPS:
  - but then performance limitation for large datasets,
  - changes from a well known HTTP address to HTTPS – user confusion?
- HTTP Digest
  - Not secure enough
- What about SOAP?
  - An invasive approach which would change the interfaces breaking existing client tools
  - Unsuited to large dataset transfers

Coupled Model Intercomparison Project Phase 5

- CMIP5 is a framework for co-ordinated climate change experiments
- Will input into the IPCC 5th Assessment Report (AR5) scheduled for 2013

20 modelling centres	mid-2009: • Simulations Starting
50 numerical experiments	2009: • Model and Simulation Documentation needed
86 simulations (total ensemble members) within experiments	end of 2010: • Data available
6500 years of simulation	early to mid 2012: • Scientific Analysis, Paper Submission and Review
Data to be available from "core-nodes" and "modelling-nodes" in a global federation.	
Users need to find & download datasets, and discriminate between models, and between simulation characteristics.	early 2013!: • Reports

- Software infrastructure under development:

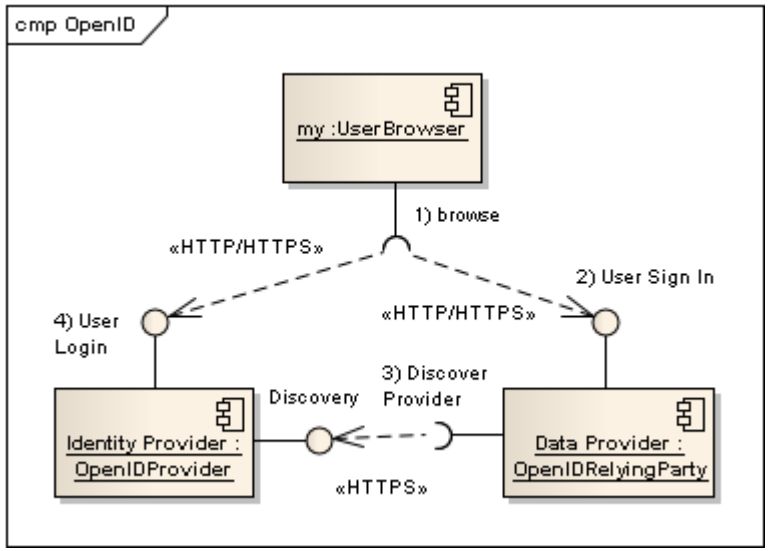
Earth System Grid

InfraStructure for the European Network for Earth System Modelling
is-enes

metafor

Earth System Curator

Earth System Grid Security: Single sign on



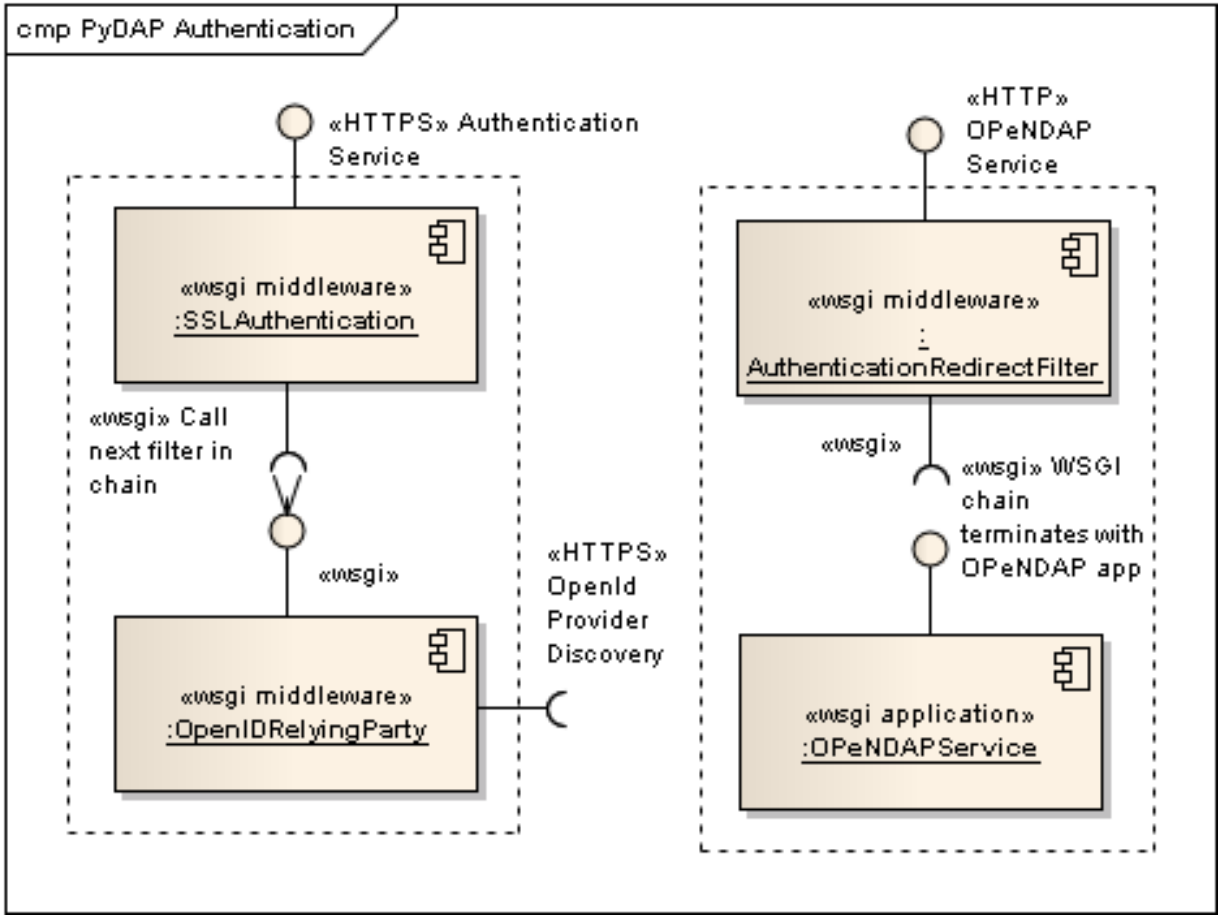
OpenID

- Users have an identity URI:
  - Identifies them and
  - an **OP** (**OpenID *Provider***), a service where they can be authenticated
- An **OpenID *Relying Party*** trusts the authentication assertion of a given OP
- SSL for mutual authenticate and enable RPs to whitelist trusted OPs

MyProxy
Credential Management Service

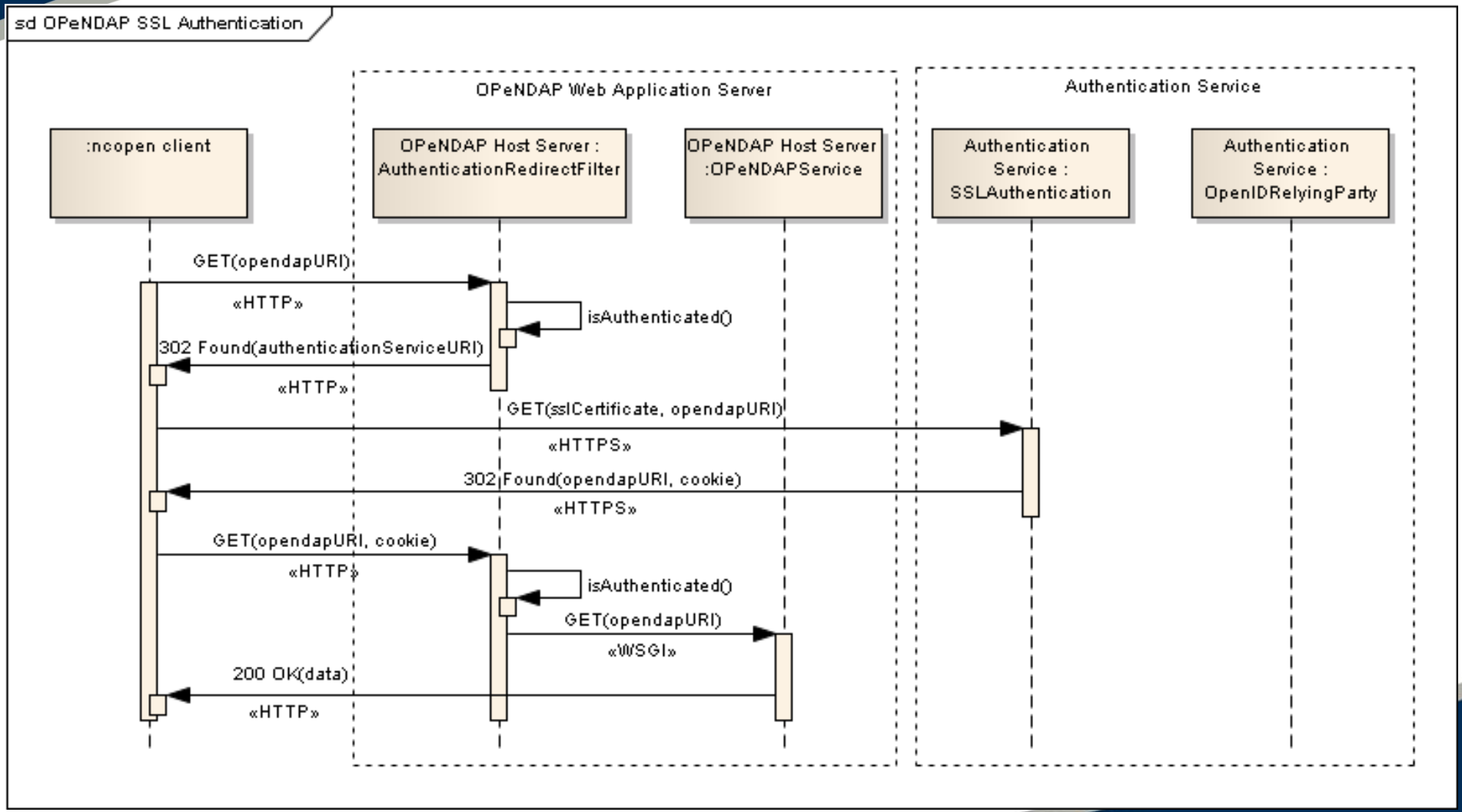
- OpenID less suited to non-browser based clients
- PKI based authentication - Grid based applications, OPeNDAP clients? ...

Filter Architecture



- OPeNDAP service is protected by an Authentication filter
- This redirects unauthenticated requests to an authentication service
- Authentication Service receives the client request
  - SSL client certificate based or
  - Default to OpenID based sign in

Filters in Action – ncopen client



More About Clients

- A server-side solution but what about the client side?
  - Browser
  - WGet and Curl – replacement to legacy ftp
  - NetCDF ncopen - patch
- Demo:
  - Browser based access
  - Command line access with wget